

THE HONORABLE ROBERT S. LASNIK

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,) No. CR19-159-RSL
Plaintiff,)
v.)
PAIGE THOMPSON,)
Defendant.)
) **REPLY IN SUPPORT OF
DEFENDANT'S MOTION TO
STRIKE CRYPTOCURRENCY
MINING ALLEGATIONS AND TO
SEVER COUNT 8**
)

In its response to Ms. Thompson’s motion to strike the cryptomining allegations in Count 1 and to sever Count 8, the government now claims, for the first time since the inception of the case, that cryptocurrency mining “is central to the government’s theory” of its case. (See Gov’t Opposition (“Opp.”) Dkt. 138 at 10.) This is an acknowledgement that the government’s wire fraud case suffers from serious legal and factual issues, namely, proof of intent to deceive and cheat as required by *United States v. Miller*, 953 F.3d 1095 (9th Cir. 2020). In lieu of such proof, the government wants to substitute evidence of Ms. Thompson’s alleged cryptomining operations (which it claims caused an uncertain amount of damages to the alleged victims, though the government has provided no evidence of such “damage” to date).

It is common knowledge that the driving force behind Ms. Thompson's prosecution is alleged access to a large volume of personal identifying information ("PII") from Capital One's rented AWS servers. That conduct is what brought Ms. Thompson to the attention of law enforcement, and it has been the government's

1 primary focus throughout the case. The government's challenge, however, is that Ms.
 2 Thompson is accused of accessing the company's public-facing server, which was
 3 mistakenly configured by Capital One to provide all of the credentials anyone needed to
 4 download this information. Although the government now attempts to portray the
 5 innocuous programming commands (which would have been rejected by any properly
 6 configured AWS server) as "steal[ing]" credentials for nefarious purposes, Capital
 7 One's server simply operated as it was configured to do because Capital One (not Ms.
 8 Thompson) allowed anyone with a proxy server and a basic understanding of AWS
 9 server commands Identity and Access Management ("IAM") roles access its servers.
 10 (See Opp. at 2-4.)

11 As the government is forced to admit, the commands "iam/info" and
 12 "iam/security credentials[role]" were not unique to a particular user, but default and
 13 publicly-known commands used to interact with the AWS platform. (*Id.*) The
 14 government further admits that Ms. Thompson did not "steal" the specific role named
 15 "****-WAF-ROLE" by entering a unique credential but rather "discovered a role" in
 16 response to use of default commands used on the AWS platform. (*Id.*) By the
 17 government's own admission, no credentials were stolen; rather, they were freely given
 18 to Ms. Thompson by virtue of the setting Capital One utilized on its web application
 19 firewall.

20 The government also has to acknowledge that Ms. Thompson used the freely-
 21 given IAM role to "sync" buckets of data to her personal computer. (*Id.* at 6.) Missing
 22 from the government's contentions, however, is any allegation that Ms. Thompson
 23 knew what she was "syncing" in advance. (See *id.*) It is hard to prove intent to deceive
 24 and cheat when the person allegedly deceiving and cheating does not even know what
 25 they've taken from what, for all intents and purposes, is a public repository of
 26 information. That is especially true here where, by Capital One's own admissions, Ms.

1 Thompson has never attempted to monetize the data¹ and the data itself has no value.²
 2 Without being able to prove Ms. Thompson illegally accessed Capital One's server or
 3 had any fraudulent intent with respect to the PII that was subsequently downloaded, the
 4 government's theory of fraud with respect to Capital One fails as a matter of law and
 5 fact.

6 The government's solution for such failings is to offer unsubstantiated
 7 allegations of cryptomining to provide its missing fraudulent intent. By adding
 8 allegations of "cryptojacking," the government hopes to confuse the jury into assigning
 9 Ms. Thompson the necessary criminal intent. Yet neither the government nor any third
 10 party subpoenaed by Ms. Thompson has produced hard evidence that Ms. Thompson
 11 engaged in any improper use of AWS computing power for cryptomining.³ The
 12 government should not be allowed to fuse these disparate theories, each lacking on their
 13 own, to impermissibly confuse the jury and obtain a conviction. The Court should strike
 14 the crypto-mining allegation in Count 1 and sever Count 8.

15 //

16 //

17 ¹ The government, on one hand, claims that Ms. Thompson, "possessed stolen
 18 information with the intent to defraud, including by obtaining counterfeit credit or debit
 19 cards," but then, on the other hand, states that it will "introduce evidence that
 20 Thompson appears to have taken steps in this direction." (Opp. at 10.) The defense has
 21 seen no credible evidence of this and the government has not provided it to the Court.
 22 Capital One has repeatedly stated that there is "no evidence that Thompson misused any
 23 of the stolen data." (Dkt. 121-1 at 12); "Capital One is aware of no evidence that she
 24 distributed the Consumer Information in any way." (Dkt. 147 at 3.)

25 ² Capital One has stated that its customers' PII has no independent monetary value
 26 unless it is used to cause a cognizable injury. (Dkt. 155-2 at 29.)

27 ³ The government has produced no evidence that AWS servers belonging to any of the
 28 alleged victims were used to mine Ethereum, which has forced Ms. Thompson to seek
 29 "bills and invoices from AWS" to attack the government's unsupported allegation.
 (Dkt. 111 at 3.)

1 **A. The Court Should Strike the Cryptomining Allegations from Count 1**
 2 **Because They are Irrelevant, Inflammatory, and Prejudicial.**

3 In its opposition, the government erroneously claims that Ms. Thompson “engaged
 4 in a scheme to defraud AWS customers and AWS in two separate ways that had a
 5 common nucleus of fact.” (Opp. at 9.) But the allegation that Ms. Thompson utilized
 6 AWS servers for cryptomining has *nothing, whatsoever, to do with* whether she might
 7 have utilized misconfigurations in an alleged victim’s web application firewalls to
 8 access stored data without authorization. This should be patently clear because neither
 9 the original indictment nor the superseding indictment list AWS as a victim. The
 10 government’s need to supersede yet again, not to add charges or victims but to restate
 11 facts, evidences how thin the government’s evidence of intent on Count 1 really is.

12 The Court should stop giving the government new ways to bite at the same apple
 13 and should strike the cryptomining allegations from Count 1—either the government
 14 can prove beyond a reasonable doubt that Ms. Thompson had the requisite intent to
 15 deceive and cheat the alleged victims to deprive them of property, *United States v.*
 16 *Miller*, 953 F.3d 1095, 1101 (9th Cir. 2020), or it cannot. It should not be permitted to
 17 use an unrelated activity as a stalking horse for intent.

18 Additionally, the government’s opposition creates a “convergence” problem. *See*
 19 *United States v. Holmes*, No. 5:18-cr-00258-EJD, 2020 WL 666563 *15-19 (N.D. Cal.
 20 Feb. 11, 2020) (dismissing wire fraud counts to the extent they depend on insured and
 21 non-paying patient-victims for lack of convergence.) The government’s new allegations
 22 that Ms. Thompson engaged in a singular scheme to defraud AWS customers and AWS
 23 in “two separate ways that had a common nucleus of fact” rest on the common nucleus
 24 of Ms. Thompson’s use of, “proxy scanner to identify AWS customers with
 25 misconfigured firewalls.” (Opp. at 9.) The government now claims that Ms. Thompson
 26 used the proxy scanner “to steal customer data and copy it to Thompson’s computer”

1 and also “to create new virtual servers and use them to mine cryptocurrency for [Ms.
 2 Thompson’s] benefit.” (*Id.*)

3 For these, “two separate ways,” to “converge,” the government must allege that
 4 she had the requisite intent, *i.e.*, “[the intent] to obtain money or property from the one
 5 who is deceived.” *United States v. Lew*, 875 F.2d 219, 221 (9th Cir. 1989); *see also*
 6 *United States v. Ali*, 620 F.3d 1062, 1071 (9th Cir. 2010) (“[U]nder *Lew*, Microsoft
 7 must be the victim from whom property was taken.”). The superseding indictment fails
 8 to allege that any of the alleged victims of cryptomining (which, to date, are Victims 7
 9 and 8) paid for Ms. Thompson’s use of their servers when she allegedly used them to
 10 mine cryptocurrency or that they were deprived of property as a result of her
 11 cryptomining.

12 The superseding indictment’s failure to make such an allegation, like its failure
 13 to identify AWS as a victim, makes plain that these are not part and parcel of one wire
 14 fraud scheme, but are distinctly different activities that the government has latched on
 15 to not because they operate around a “common nucleus of fact,” but because the
 16 government is attempting to impermissibly circumvent its burden of proof at trial.

17 The cryptomining allegation is not “central” to the government’s fraud theory and
 18 serves solely to confuse, prejudice, and inflame the jury into believing that Ms.
 19 Thompson was a bad actor who must have possessed the requisite intent to defraud the
 20 alleged victims, even if the government cannot otherwise prove the actual deprivation
 21 of property or harm. As such, reference to it should be stricken from Count 1 and the
 22 government should not be permitted to save its flawed theory with a second superseding
 23 indictment.

24 //

25 //

26 //

1

2 **B. The Court Should Sever Count 8 Because there is No Evidence that Ms.**

3 **Thompson Used Servers Belonging to Victims 7 and 8 to Cryptomine and**

4 **No Evidence that Their Computers Were Damaged in Excess of \$5,000.**

5 The government's response as to why it has failed to provide Ms. Thompson

6 with any evidence to prove the unsubstantiated allegations in Count 8, namely that Ms.

7 Thompson's cryptomining harmed Victims 7 and 8 in excess of \$5,000, is as follows: it

8 is Ms. Thompson's fault because she "designed her cryptocurrency mining activity to

9 be hard to detect." (Opp. at 14.) That is a plainly ridiculous response—we are less than

10 three months from trial, either the government has the evidence to prove up its

11 allegations or it does not. Given the government has provided no evidence to the

12 defense—or to this Court—to substantiate Count 8, the Court should order an

13 evidentiary hearing to determine whether the government *actually* has evidence to

14 substantiate this charge or whether it is using it, as the defense surmises, as a stalking

15 horse for intent on the CFAA charges. This should be done before the government

16 returns a second superseding indictment to attempt to fix the serious flaws in its

17 charges.

18 As *Van Buren v. United States* made clear, the CFAA does not impose liability for

19 someone having "improper motives" for accessing a computer that is otherwise

20 available to them. 141 S. Ct. 1648, 1652 (2021). The only intent relevant under the

21 CFAA is the intent in accessing the computer system, not the actions that occur after

22 such access occurs. *See id.* Thus, whether Ms. Thompson mined cryptocurrency or not

23 is thoroughly irrelevant to all of the CFAA charges save for Count 8. Federal Rules of

24 Criminal Procedure 8 and 14 provide the Court the ability to "order separate trials of

25 counts" or "provide any other relief that justice requires" where joinder of offenses in

26 an indictment "appears to prejudice a defendant." Such actions are thoroughly

warranted here.

1 Permitting the government to proceed forward with Count 8 would have a
 2 “substantial and injurious effect or influence” on the verdict and would cause Ms.
 3 Thompson “manifest prejudice.” *United States v. Jawara*, 474 F.3d 565, 579 (9th Cir.
 4 2007). Although the government suggests that any prejudice could be cured by limiting
 5 instructions to consider each count separately, such limiting instructions would not cure
 6 the prejudice in this case, where the government is conflating the evidence of “data
 7 theft” and “cryptomining” in both the wire fraud and CFAA allegations to substitute for
 8 the factual defects in its case.

9 It is not that Ms. Thompson believes a jury would be unable to understand the
 10 technical underpinnings of cryptomining, (Opp. at 13), is it that it would be
 11 impermissibly confused as to the intent required for both wire fraud and the CFAA
 12 charges because of the government’s commingling of the two. *See United States v.*
 13 *Johnson*, 820 F.2d 1065, 1070 (9th Cir. 1987) (stating severance is necessary where
 14 “jury may cumulate the evidence of the various crimes charged and find guilt when, if
 15 considered separately, it would not so find”).

16 The evidence against Ms. Thompson under Count 8 is non-existent even though
 17 the “government [claims it] has provided full discovery.” (Dkt. 131 at 3.) Victims 7 and
 18 8, the identified entities relevant to Count 8 have been identified. (Ex. 1, AUSA Letter
 19 dated June 22, 2021 (filed under seal).) Victim 7 represented to the government that
 20 they have, “no indication that the unauthorized usage [of their servers] involved
 21 cryptocurrency mining.” (Ex. 2,⁴ FBI 302; Ex. 3, E-mails (filed under seal).) Victim 8
 22 also represented to the government that they were “unaware of any associated
 23 cryptocurrency mining, but offered to conduct more research and update writer with
 24 any additional findings.” (Ex. 3, FBI 302 (filed under seal).) Count 8 either needs to be

25

 26 ⁴ Ms. Thompson would have filed Exhibits 2 through 4 with her opening motion;
 however, she could not because the government did not disclose them until after she
 filed the motion.

severed and the government ordered to produce relevant discovery, or the Court should hold an evidentiary hearing to determine what evidence, exactly, the government intends to introduce at trial so that it can determine, for itself, whether a limiting instruction would truly cure the prejudice caused by the government's inclusion of Count 8.

* * *

For all the reasons set out in this reply and Ms. Thompson’s motion, the Court should exercise sound discretion striking the cryptomining allegations in Count 1 and severing Count 8.

DATED: January 10, 2022.

Respectfully submitted,

/s/ Mohammad Ali Hamoudi
MOHAMMAD ALI HAMOUDI
/s/ Christopher Sanders
CHRISTOPHER SANDERS
/s/ Nancy Tenney
NANCY TENNEY
Assistant Federal Public Defenders

/s/ Brian Klein
BRIAN KLEIN
/s/ Melissa Meister
MELISSA MEISTER
Waymaker LLP

Attorneys for Paige Thompson